1. Record Nr. UNISA996465505403316

Titolo	Cryptography and Coding [[electronic resource]] : 14th IMA International Conference, IMACC 2013, Oxford, UK, December 17-19, 2013, Proceedings / / edited by Martijn Stam
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-45239-6
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XII, 365 p. 39 illus.)
Collana	Security and Cryptology ; ; 8308
Disciplina	005.82
Soggetti	Data encryption (Computer science) Coding theory Information theory Algorithms Data structures (Computer science) Computer security Computer science—Mathematics Cryptology Coding and Information Theory Algorithm Analysis and Problem Complexity Data Structures and Information Theory Systems and Data Security Discrete Mathematics in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Bits and Booleans -- Semi-bent Functions from Oval Polynomials -- Efficient Generation of Elementary Sequences -- Homomorphic Encryption -- On the Homomorphic Computation of Symmetric Cryptographic Primitives -- Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme -- On the Relationship between Functional Encryption, Obfuscation and Fully Homomorphic Encryption -- Codes and Applications -- On Minimal and Quasi-minimal Linear Codes -- A Code-Based Undeniable Signature Scheme -- Cryptanalysis

-- Filtered Nonlinear Cryptanalysis of Reduced-Round Serpent and the Wrong-Key Randomization Hypothesis -- Differential Cryptanalysis of Keccak Variants -- Recovering Private Keys Generated with Weak PRNGs -- Protecting against Leakage -- A Leakage-Resilient Pairing-Based Variant of the Schnorr Signature Scheme -- High-Order Masking by Using Coding Theory and Its Application to AES -- Hash Functions -- Hashing Mode Using a Lightweight Blockcipher -- Indifferentiability of Double Length Compression Functions -- Security Amplification against Meet-in-the-Middle Attacks Using Whitening -- Key Issues -- Secure Key Management in the Cloud -- Estimating Key Sizes for High Dimensional Lattice-Based Systems -- Sub-linear Blind Ring Signatures without Random Oracles -- Constructions of Signcryption in the Multi-user Setting from Identity-Based Encryption -- Anonymous Constant-Size Ciphertext HIBE from Asymmetric Pairings.

Sommario/riassunto

This book constitutes the proceedings of the 14th IMA International Conference on Cryptography and Coding, IMACC 2013, held at Oxford, UK, in December 2013. The 20 papers presented were carefully reviewed and selected for inclusion in this book. They are organized in topical sections named: bits and booleans; homomorphic encryption; codes and applications; cryptanalysis; protecting against leakage; hash functions; key issues and public key primitives.